UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X	MEMORANDUM
IN RE GRAND JURY	AND ORDER
SUBPOENA TO [REDACTED,] INC.	
----------X	18-MC-0334 (JO)

James Orenstein, Magistrate Judge:

The government seeks an order requiring the recipient of a subpoena not to notify any person of the existence of the subpoena for a period of one year. For the reasons set forth below, I deny the government's motion.

I assume the reader's familiarity with the relevant statutory scheme that authorizes a court, under certain circumstances, to grant the kind of relief the government now seeks. *See*, *e.g.*, *In re Grand Jury Subpoena to Google Inc.*, 2017 WL 4862780, at *1 (E.D.N.Y. Oct. 26, 2017) ("*Google EDNY*"); *In re Grand Jury Subpoena to Facebook*, 2016 WL 9274455, at *1 (E.D.N.Y. May 12, 2016); *In re Search Warrant Issued to Google, Inc.*, 269 F. Supp. 3d 1205, 1208 (N.D. Ala. 2017). Briefly stated, when a warrant, subpoena, or court order is issued to "a provider of electronic communications service or remote computing service" (which I shall call a "service provider" for ease of reference), the court "shall" order the service provider not to disclose its existence if the court "determines that there is reason to believe that notification … will result in" any of several adverse consequences to a criminal investigation or trial. 18 U.S.C. § 2705(b).

In the instant matter, the grand jury has issued a subpoena to an entity that the government describes – using the kind of boilerplate language it routinely uses in such circumstances – as "a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote comput[ing] service, as defined in 18 U.S.C. § 2711(2)." Docket Entry ("DE") 1 (Application) at 1. The government provides no other information about the entity. The government goes on to explain the basis for the required factual finding as follows:

> In this case, [the requested] order would be appropriate because the attached subpoena relates to an ongoing criminal investigation that is neither public nor known to targets of the investigation, and there is reason to believe that its disclosure will alert targets to the ongoing investigation. Specifically, the account listed in the subpoena is believed to be used by an individual who is the target of the investigation, who is at large, and who does not yet know of the investigation. Accordingly, there is reason to believe that notification of the existence of the attached subpoena will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b). Some of the evidence in this investigation is stored electronically and can be completely and permanently erased. Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the subpoena, there is reason to believe that the targets under investigation will destroy that evidence and change their patterns of behavior.

Application at 1-2.

There are several reasons I cannot issue the requested order based on the existing record. First, it is not clear from the face of the Application that the subpoenaed entity is actually the kind of service provider that the statute regulates. To be sure, the government makes a conclusory assertion that it is one "and/or" the other of the two types of providers to which the statute refers, but it provides no information that would allow me to assess that assertion. Were the subpoena directed to a well-known company such as Google or Facebook, each of which plainly fits the pertinent definitions, I would not hesitate in this regard. But as explained below, I cannot simply rely on the government's conclusory assertion on this issue. The government has previously taken the position, for example, that a cruise ship company is a covered service provider because it furnishes Wi-Fi service to its guests. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 17-MC-2682 (DAR), DE 2 (Memorandum and Order) (D.D.C Nov. 29, 2017). Such a theory would apply with equal force to many stores, restaurants, schools, and individual homeowners – none of which could plausibly be considered a service provider within the law's

meaning. *See id.* at 2-3 & n.2.[1] It is thus apparent that the government is willing to read the definitional provisions of the Stored Communications Act so expansively that a court should be wary of accepting at face value a conclusory assertion that the statute applies to a given entity about which no additional information is provided.

Second, even assuming that the entity is indeed a covered service provider – as is plausible, given the subpoena recipient's corporate name and the fact, mentioned in the subpoena itself but not in the Application, that the "account" to which the subpoena is directed is an email account – I have no way to determine if the account at issue is in fact associated in any way with the investigative target.[2] The government writes only that "the account listed in the subpoena is believed to be used by … the target of the investigation."[3] The government discloses neither the identity of the person – investigative agent or prosecutor – who holds such a belief nor the facts upon which

[1] The government has objected to the magistrate judge's conclusion that the cruise ship company is not a covered service provider, and the district judge's review of the decision remains pending. Briefing will be completed by February 19, 2018. *See In re Application*., Minute Order dated Jan. 12, 2018. While the district judge in that case may ultimately disagree with the magistrate judge's analysis, I find it persuasive.

[2] Further complicating the task, it is unclear if the government, in referring to "targets," is using the term's formal definition to refer to a putative defendant, *see* U.S. Attorney's Manual § 9-11.151 (defining "target" as "a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant"), or is merely using a colloquialism that connotes a person who would more precisely be defined as an investigative "subject." *See id.* ("a person whose conduct is within the scope of the grand jury's investigation"). Either usage would be entirely plausible – and the distinction matters if I am to determine whether it is reasonable to believe that the person being described would have an incentive to engage in obstructive conduct (even assuming that the person is unaware of the investigation and therefore of his or her status).

[3] Adding still more reason to conclude that the government has provided formulaic boilerplate devoid of any actual information that would help resolve the factual issue before the court, the quoted phrase appears to suggest that the person believed to be associated with the subpoenaed information is "the" target of the investigation – which seems inconsistent with other references in the same paragraph to multiple "targets" of that same investigation.

that belief is predicated. *See Google EDNY*, 2017 WL 4862780, at *2 (noting same problem in earlier application). As with the government's assertion that the subpoenaed entity is a covered service provider, I am asked to accept on faith the unidentified government employee's professed belief.

Indeed, the government does not even explain whether, in using the passive voice once again to assert that the account "is used by … the target," it means that the target is the account subscriber, or if instead that phrasing connotes some more attenuated connection between the target and the account. Here, too, the imprecision matters: if the target is the account's subscriber (under either a true name or an alias), then in the absence of a nondisclosure order it may be likely that the subpoena recipient will notify the target of the subpoena's existence (although the government has similarly provided no information supporting that assumption). But if the target is not the subscriber, and merely uses the account in some unspecified way, then I would need to know about the nature and extent of the usage, and the relationship between the subscriber and the target to be able to make in good faith the factual finding that allowing the company to notify its customer of the subpoena would eventually lead to the target's acquisition of such notice, and thence to the obstructive conduct the government fears.

Beyond its belief that the target somehow uses the email account at issue, the government engages in pure speculation about the potential adverse consequences of disclosure. It writes that notice would give the target "an opportunity" to flee and obstruct, and that is undoubtedly true. But it tells me nothing about whether it is reasonable to believe that the target "will" engage in such conduct, which is the question I must answer. Some context would help: if, for example, the target is being investigated on the basis of an anonymous tip for the misdemeanor of fraudulently displaying the emblem of the 4-H clubs, *see* 18 U.S.C. § 707, I might hesitate to conclude that the target of such an investigation, upon discovering his status, would either embrace the life of a fugitive or risk the

far more severe sanctions for obstruction of justice. On the other hand, I would think it entirely likely that the target of a well-predicated murder investigation might make such choices if given the chance. As the record currently stands, I can engage in no such analysis.

Similarly, the government tacitly assumes that in any investigation involving either electronically stored records or electronic communications – which is to say, in essentially every criminal investigation in which a non-disclosure order would potentially be available under Section 2705(b) – a person's awareness that she is under investigation supports a finding that she will delete or encrypt evidence so as to make it unavailable to law enforcement. Neither experience nor logic supports such a syllogism. It is of course true that the technology that allows a person to store and transmit information electronically also allows such information to be hidden or destroyed (even if it is harder to do so effectively than many targets would suspect or than the government would have me assume). But that truism, without more, does not reasonably support the conclusion that every investigative target will do so if possible.

The risk that persons who learn they are under investigation will engage in obstruction is a real one, but it arises to different degrees in different circumstances. Congress could have chosen to address that risk in blunderbuss fashion by universally prohibiting the recipient of any warrant, order, or subpoena from disclosing its existence, but it plainly chose not to do so. Nor did Congress choose to alleviate that risk either by requiring a non-disclosure order either where obstruction is merely a possibility, or by committing the discretion to secure relief to the executive branch (as it effectively did, by contrast, with respect to pen registers). Instead, it prescribed a more nuanced approach, circumscribing both the persons who could be subjected to silencing, and the circumstances in which a court may (and must) order it.

By relying on the conclusory, formulaic, and universally applicable assertions set forth in the instant Application, the government essentially seeks to negate that legislative choice and replace it with the blanket prohibition that Congress eschewed. A court cannot accede to that effort. The applicable law requires a factual finding; making such a finding requires facts. The sparse facts and speculative assertions in the Application do not suffice to allow the finding the government seeks.

It is of course entirely possible that in this case and others, applying the law as Congress wrote it will put an investigation at risk. Every investigation must start somewhere, and in the early stages of some cases the government will simply lack the information needed to secure the non-disclosure order necessary to avert a real – albeit as yet unprovable – risk of obstruction. But that concern does not allow a court to jettison an applicable legal standard. The government has not provided information that would support a finding that notification of the existence of the subpoena at issue will result in a cognizable harm to the investigation. I therefore deny the Application. I respectfully direct the Clerk to file the Application and proposed Order on the docket and maintain each under seal until May 6, 2018, subject to a 90-day extension upon a showing of continuing need for secrecy. This Memorandum and Order may be filed on the public docket, as it includes no information that can compromise the government's investigation.[4]

SO ORDERED.

Dated: Brooklyn, New York
February 5, 2018

/s/
James Orenstein
U.S. Magistrate Judge

[4] Although I do not need to reach the issue, I note that the government again, as it did in *Google EDNY*, seeks to silence a subpoena recipient for an entire year – the maximum permitted under a recent change in Justice Department policy – and seeks to have its Application and proposed order sealed indefinitely, all without explaining the need for those proposed durations. *See Google EDNY*,

2017 WL 4862780, at *4. I questioned the need in *Google EDNY* for such a lengthy restriction of the subpoena recipient's speech and secrecy, ordered the application sealed for 90 days (with a 90-day extension available upon a showing of continued need), and "respectfully request[ed] that in all future sealing requests, the government submit proposed orders with a similar temporal limitation absent a showing of need to do otherwise." *Id.* *5 & n.3. I respectfully remind the government of the request it has thus far ignored and invite it to treat the request as a directive in the future; should that prove ineffective, I will consider more effective measures to avoid needless secrecy.